IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.	:	10/786,224	Confirmation No.	:	2832
First Named Inventor	:	Burkhard KUHLS			
Filed	:	February 26, 2004			
TC/A.U.	:	2136			
Examiner	:	JOHNSON, CARLTON			
Docket No.	:	080437.53236US			
Customer No.	:	23911			
Title	:	Method for Providing Software to Be Used by a Control Unit of a Vehicle			

PRE-APPEAL BRIEF CONFERENCE REQUEST

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to the Official Gazette noticed dated July 12, 2005, Applicant respectfully submits that the rejections of record are clearly not proper and without basis. As will be described in detail below, this Request is based on the fact that the Patent Office has not provided sufficient evidence to support a *prima facie* case of obviousness.

The Rejection of Claims 1-20 for Obviousness in View of the Combination of U.S. Patent No. 5,957,985 to Wong et al. ("Wong") and U.S. Patent No. 6,463,535 to Drews ("Drews") is Improper

The fundamental issue of this Request is whether the Patent Office has provided sufficient evidence to prove that the combination of Wong and Drews renders obvious Applicant's claimed method that involves *signing software* against falsification. Specifically, Applicant's claim 1 recites a method that involves *software* that is:

- signed against falsification;

- signed using a secret key; and

- checked for integrity using a public key complimentary to the secret key.

The Office Action acknowledges that Wong does not disclose or suggest the use of signed software, and instead relies upon Drews for this disclosure. Drews, however, does not disclose or suggest signing software. Instead, Drews discloses *signing a set of hash values* generated from a boot image.

The Set of Hash Values of Drews is Not Software

The boot image of Drews comprises one or more sub-images[1]. Each sub-image is loaded into a one-way hash function to produce a hash value[2]. A number of hash values are appended end-to-end to produce a hash set, and this hash set is digitally signed[3]. Thus, unlike the method of Applicant's claim 1 which involves *signed software*, Drews discloses the use of a *signed hash set*, which is referred to in Drews as the manifest digital signature.

A platform can download the boot image and the manifest digital signature. The manifest digital signature is decrypted to produce a *hash value* that is compared to a *hash value* calculated for the downloaded boot image[4]. Thus, it cannot be disputed that Drews only discloses *signing a set of hash values* created from the boot image, and there is no disclosure or suggestion of actually signing the boot image itself.

It is significant that the hash function used by Drews is a one-way hash function. As disclosed by Drews, one-way hash functions are designed such that "there does not readily exist an inverse function to recover any discernible

[1] Column 3, lines 16-18.
[2] Column 4, lines 38-42.
[3] Column 4, lines 45-50.
[4] Column 5, lines 46-58.

portion of the boot image from the hash value.[5]" Accordingly, it is not possible to recreate the boot image from the hash values, and these hash values are merely a numerical derivation of the boot image.

Because it is not possible to recreate the boot image from the hash values, it cannot be said that signing the hash values is the same as signing the boot image. In other words, the hash function *transforms* the boot image into something else, namely a set of hash values. Thus, Drews does not disclose signing the boot image itself, and the signed set of hash values cannot be interpreted as software. In view of the above, it is clear that there is nothing in Drews disclosing or suggesting signing software, signing software using a private key, or checking the integrity of the signed software using a public key that is complimentary to the private key.

As set forth in Applicant's Reply dated January 14, 2008, none of the citations to Drews set forth in the Office Action contradicts the arguments above that Drews only discloses signing a set of hash values. In fact, the Advisory Action acknowledges that Drews only discloses signing a set of hash values. The Advisory Action, however, without providing any type of reasoning or other evidence, concludes that signing the hash set is the same as signing the boot image. Mere conclusions, unsupported by any reasoning or other evidence, cannot be the basis of the *prima facie* case of obviousness. Accordingly, the Patent Office has not met its initial burden of providing evidence that the use of *signed software* in the manner recited in Applicant's claims is obvious.

[5] Column 4, lines 42-44.

The Combination of Wong and Drews Does Not Disclose or Suggest the Specific Certificates Recited in Claim 7

The Patent Office bears the initial burden of presenting evidence in order to establish a *prima facie* case of obviousness. The rejection of Applicant's claim 7, however, provides no such evidence that the specific certificates recited in this claim are disclosed or suggested by the combination of Wong and Drews.

Applicant's claim 7 recites a clearing code site signature certificate and a software signature certificate. The final Office Action provides a definition of a certificate and appears to rely upon the certificate chain 320 of the signed manifest 150 as disclosing these specific certificates[6]. The final Office Action does not provide any evidence or reasoning as to why this generic disclosure of certificates renders obvious the specific certificates recited in Applicant's claim 7. Without such evidence or reasoning, the Patent Office has not met its burden to establish a *prima facie* case of obviousness.

Conclusion

Because the Patent Office has not provided any evidence of the use of signed software in the manner recited in Applicant's claims, or the specific certificates recited in Applicant's claim 7, the Patent Office has not met its burden in providing such evidence to establish a prima facie case of obviousness.

[6] It is noted that the definition of a certificate provided in the Office Action does not appear to be consistent with the definition provided in column 2, lines 59-66 of Drews.

If there are any questions regarding this response or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

If necessary to effect a timely response, this paper should be considered as a petition for an Extension of Time sufficient to effect a timely response, and please charge any deficiency in fees or credit any overpayments to Deposit Account No. 05-1323 (Docket # 080437.53236US).

Respectfully submitted,

February 20, 2008

Stephen W. Palan
Registration No. 43,420

CROWELL & MORING, LLP
Intellectual Property Group
P.O. Box 14300
Washington, DC 20044-4300
Telephone No.: (202) 624-2500
Facsimile No.: (202) 628-8844
SWP:crr
4973063